PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-111671
(43)Date of publication of application : 30.04.1996

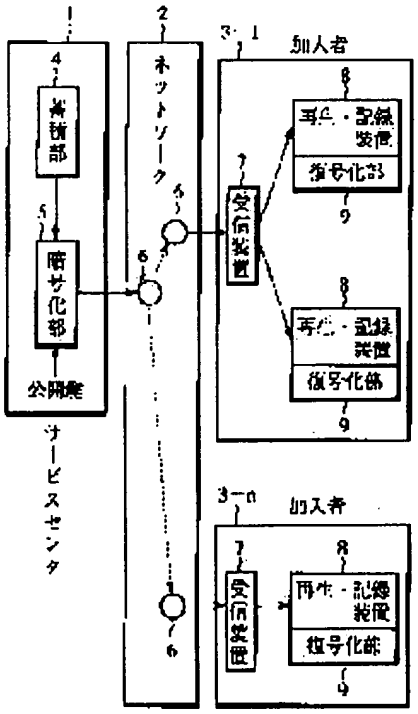
(51)Int.Cl. H04H 1/00
G09C 1/00
H04L 9/06
H04L 9/14
H04L 12/54
H04L 12/58

(21)Application number : 06-247468
(22)Date of filing : 13.10.1994

(71)Applicant : FUJITSU LTD
(72)Inventor : NAKAJIMA ICHIRO
ISHIHARA TOMOHIRO
TANAKA ATSUSHI
OKUDA MASAHITO

(54) DATA DISTRIBUTION SYSTEM

(57)Abstract:
PURPOSE: To prevent the unauthorized copy on the side of a subscriber, regarding a data distribution system distributing data to the subscriber from a service center via a network.
CONSTITUTION: A service center 1 is provided with a storage part 4 storing various kinds of data and reading the data according to the requests from subscribers 3-1 to 3-n and a ciphering part 5 ciphering data by the open keys corresponding to the secret keys of the subscribers and transmitting the data. The reproducing/recording device 8 such as personal computers, etc., of the subscribers 3-1 to 3-n has a decoding part 9 where the secret keys are preliminarily set, decodes ciphered data in the decoding part 9 only when the ciphered data received from the node 6 of a network 2 by a receiver 7 is reproduced and displayed, and records the ciphered data as it is when the recording is performed.



LEGAL STATUS

[Date of request for examination] 22.12.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－111671

(43)公開日　平成８年(1996)４月30日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｈ　1/00	Ｎ			
Ｇ０９Ｃ　1/00		7259－5Ｊ		
Ｈ０４Ｌ　9/06				
			Ｈ０４Ｌ　9/ 02　Ｚ	
		9466－5Ｋ	11/ 20　１０１　Ｂ	

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平6－247468

(22)出願日　平成６年(1994)10月13日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　中島　一郎
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　石原　智宏
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　田中　淳
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人　弁理士　柏谷　昭司　（外１名）

最終頁に続く

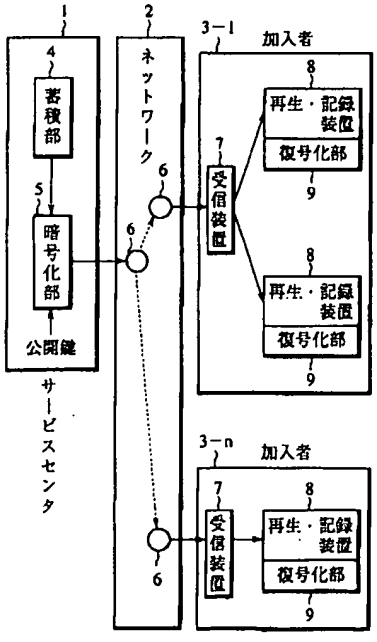
(54)【発明の名称】　データ分配システム

(57)【要約】

【目的】　サービスセンタからネットワークを介して加入者にデータを配信するデータ分配システムに関し、加入者側に於ける無断複製を防止する。

【構成】　サービスセンタ１は、各種のデータを蓄積し、加入者３－１～３－ｎからのリクエストに応じたデータを読出す蓄積部４と、加入者の秘密鍵に対応した公開鍵でデータを暗号化して送出する暗号化部５とを備える。又加入者３－１～３－ｎのパソコン等の再生・記録装置８は、予め秘密鍵が設定された復号化部９を有し、ネットワーク２のノード６から受信装置７で受信した暗号化データを再生表示する時のみ復号化部９で復号化し、記録する時は暗号化データのまま記録する。

本発明の原理説明図



【特許請求の範囲】
【請求項１】　音声データ，文字等のコードデータ，静止画等のイメージデータ等の各種のデータを蓄積した蓄積部を備えたサービスセンタから、加入者のリクエストに従ったデータを、該加入者にネットワークを介して配信するデータ分配システムに於いて、
前記サービスセンタは、前記加入者のリクエストに従って選択したデータを前記蓄積部から読出し、該加入者の秘密鍵に対応する公開鍵によって暗号化して配信する構成を備え、
前記加入者は、前記公開鍵で暗号化されたデータを受信して記録し、再生時のみ、予め設定された秘密鍵で復号化して表示する構成の再生・記録装置を備えたことを特徴とするデータ分配システム。
【請求項２】　前記ネットワークの前記加入者を収容したノードは、前記サービスセンタからのデータをコピーし、同一の複数のデータについてそれぞれ加入者の秘密鍵に対応する公開鍵で暗号化してリクエストを行った加入者に配信する構成を備えたことを特徴とする請求項１記載のデータ分配システム。
【請求項３】　前記サービスセンタは、同一のデータに対する単一又は複数の加入者からの複数のリクエストについて、該データとリクエスト数とを前記ネットワークの前記加入者を収容したノードに転送し、該ノードは、前記サービスセンタからのデータを前記リクエスト数に従った数だけコピーし、それぞれ前記加入者の秘密鍵に対応する公開鍵で暗号化してリクエストを行った加入者に配信する構成を備えたことを特徴とする請求項１記載のデータ分配システム。

【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、サービスセンタに蓄積した各種のデータを、加入者のリクエストに従ってネットワークを介して配信するデータ分配システムに関する。マルチメディアサービスについては既に各種の方式が提案されている。又ネットワークの高度化が進められており、このネットワークを介して各種のデータを加入者に配信するシステムが考えられる。その場合に、著作権の問題があり、無断複製を防止する手段が必要となる。
【０００２】
【従来の技術】図５は従来例の説明図であり、５１はサービスセンタ、５２はネットワーク、５３－１～５３－ｎは加入者、５４は蓄積部、５５は公開鍵等による暗号化部、５６は秘密鍵等による復号鍵により復号する復号化部、５７は受信装置、５８は再生・記録装置である。又加入者５３－１は、パーソナルコンピュータ等の１台の再生・記録装置５８を備え、又加入者５３－ｎは複数台の再生・記録装置５８を備えた場合を示す。
【０００３】サービスセンタ５１に暗号化部５５を備えていない場合は、加入者５３－１～５３－ｎに於いても復号化部５６を省略できるものであり、その場合は、加入者からのリクエストをネットワーク５２を介してサービスセンタ５１に送出すると、サービスセンタ５１は、加入者の識別番号等を基に契約者等のアクセス可能の加入者であるか否かを判定し、アクセス可能の加入者の場合は、蓄積部５４を検索してリクエストに対応したデータを読出し、ネットワーク５２を介してリクエストを送出した加入者に配信する。
【０００４】この場合、サービスセンタ５１から加入者５３－１～５３－ｎに配信されるデータは、暗号化されていないので、盗聴の可能性があると共に、無断複製が容易であり、著作権の問題が生じる。
【０００５】そこで、サービスセンタ５１に暗号化部５５を設けて、蓄積部５４から読出したデータを暗号化して送出し、加入者５３－１～５３－ｎは、受信装置５７により受信し、復号化部５６に契約等によって予め設定した復号鍵を用いて復号し、再生・記録装置５８に復号されたデータを加える構成が考えられた。それにより、契約者以外は、サービスセンタ５１にアクセスして、暗号化されたデータを受信しても復号できないので、著作権の保護が可能となる。
【０００６】
【発明が解決しようとする課題】加入者が１台の再生・記録装置５８を所有している場合は余り問題はないが、加入者５３－ｎのように、複数台の再生・記録装置５８を所有している場合は、復号化部５６で復号されたデータをそれぞれの再生・記録装置５８に加えて、記録又は再生することができる。従って、復号化部５６で復号された後は無断複製が可能となり、著作権の問題が生じる。特に、企業等を１加入者としたような場合に、１台の受信装置と復号化部とにより、サービスセンタ５１からの暗号化データを復号し、多数の再生・記録装置５８により記録又は再生することが可能となり、個人利用の複製ではなくなる場合が生じる。本発明は、再生時のみ復号可能とし、無断複製を防止することを目的とする。
【０００７】
【課題を解決するための手段】本発明のデータ分配システムは、図１を参照して説明すると、（１）音声データ，文字等のコードデータ，静止画等のイメージデータ等の各種のデータを蓄積した蓄積部４を備えたサービスセンタ１から、加入者３－１～３－ｎのリクエストに従ったデータを、この加入者３－１～３－ｎにネットワーク２を介して配信するデータ分配システムに於いて、サービスセンタ１は、加入者のリクエストに従って選択したデータを蓄積部４から読出して、この加入者の秘密鍵に対応する公開鍵によって暗号化して配信する構成を備え、加入者は、公開鍵で暗号化されたデータを受信して記録し、再生時のみ、予め設定された秘密鍵で復号化して表示する構成の再生・記録装置８を備えている。又５

は公開鍵で暗号化する暗号化部、６はネットワーク２のノード、７は受信装置、９は秘密鍵で復号する復号化部である。

【０００８】（２）又ネットワーク２の加入者を収容したノード６は、サービスセンタ１からのデータをコピーし、同一の複数のデータについてそれぞれ加入者の秘密鍵に対応する公開鍵で暗号化してリクエストを行った加入者に配信する構成を備えることができる。

【０００９】（３）又サービスセンタ１は、同一のデータに対する単一又は複数の加入者からの複数のリクエストについて、そのデータとリクエスト数とを、ネットワークの加入者収容のノード６に転送し、このノード６は、サービスセンタ１からのデータをリクエスト数に従った数だけコピーし、それぞれ加入者の秘密鍵に対応する公開鍵で暗号化してリクエストを行った加入者に配信する構成を備えることができる。

【００１０】

【作用】

（１）加入者３－１～３－ｎの再生・記録装置８は、復号化部９に予め定められた秘密鍵を設定して、再生時のみ復号化部９によって復号するもので、受信記録する場合は、サービスセンタ１からの暗号化データはそのまま記録する。従って、この記録データを他の再生・記録装置に転送して記録しても、再生時には秘密鍵が異なることから、復号できないことになる。即ち、契約等による特定の再生・記録装置のみが、サービスセンタ１からの暗号化データを復号して再生できるから、著作権の保護が可能となる。

【００１１】（２）又ネットワーク２のノード６に、コピー機能と暗号化機能とを設け、加入者からのリクエストに従ってサービスセンタ１の蓄積部４から読出したデータを、その加入者が収容されたノードに送出する。この場合、サービスセンタ１から暗号化しないデータを送出し、ノード６に於いて必要数をコピーし、それぞれ加入者の秘密鍵に対応した公開鍵で暗号化して配信する。従って、サービスセンタ１とネットワーク２との間のトラヒックを低減することができる。

【００１２】（３）又サービスセンタ１が同一のデータのリクエストを受けた時に、そのリクエスト数と暗号化しないデータとを、リクエストを行った加入者を収容したノード６に転送する。ノード６は、サービスセンタ１から受信したデータをリクエスト数だけコピーし、加入者の秘密鍵に対応した公開鍵でそれぞれ暗号化して配信する。

【００１３】

【実施例】図２は本発明の実施例の説明図であり、１１はサービスセンタ、１２はネットワーク、１３は加入者、１４は蓄積部、１５は暗号化部、１６はノード、１７は受信装置、１８は再生・記録装置、２０は公開鍵処理部、２１はリクエスト受付部、２２は送信部、２３は選択処理部、２４は記録部、２５は復号化部、２６は再生部、２７はリクエスト送信部である。

【００１４】サービスセンタ１１の蓄積部１４は、音声データ，文書等のコードデータ，静止画等のイメージデータ等の各種のデータを蓄積し、加入者のリクエストに応じたデータを検索して読出すことができる磁気ディスク装置，光ディスク装置，半導体大規模集積回路記憶装置等の大容量の記憶装置によって構成されている。又リクエスト受付部２１は、加入者からのデータ名と加入者番号等を含むリクエストを受付け、データ名等によって蓄積部１４を検索してデータの読出しを行い、又加入者番号等によって、加入者の秘密鍵に対応する公開鍵を公開鍵処理部２０から暗号化部１５に加えるように制御し、又送信部２２に対してリクエストを行った加入者に暗号化データを送出するように制御する。

【００１５】又暗号化部１５は、蓄積部１４から読出したデータを、公開鍵処理部２０からの公開鍵によって暗号化し、送信部２２に加えるものである。暗号化方式としては、例えば、秘密鍵暗号化方式と公開鍵暗号化方式とに分けることができ、秘密鍵暗号化方式は、同一の鍵を用いて暗号化と復号化とを行うものであり、例えば、ＤＥＳ（Data Encryption Standard）方式が知られている。又公開鍵暗号化方式としては、例えば、ＲＳＡ（Rivest，Shamir，Adleman）方式が知られている。本発明に於いては、基本的には公開鍵暗号化方式を適用するもので、前述のＲＳＡ方式は勿論のこと、それ以外の既に知られている各種の方式を適用できるものである。

【００１６】前述のＲＳＡ方式は、暗号化鍵を（ｅ，ｎ）の組とし、これに対応する復号化鍵を（ｄ，ｎ）の組とすると、ｅ，ｎは公開鍵、ｄは秘密鍵を示すものとなる。そして、データをＭ、暗号化データをＣとすると、

$$C = M^e \mod n \quad \cdots (1)$$

$$M = C^d \mod n \quad \cdots (2)$$

で表される。

【００１７】そして、ｐ，ｑをそれぞれ素数とし、

$$n = p \times q \quad \cdots (3)$$

の関係とし、（ｐ－１）と（ｑ－１）との最小公倍数Ｌを求め、この最小公倍数Ｌと互いに素で、これより小さい任意の整数をｅ（１＜ｅ＜Ｌ）とする。そして、この整数ｅと最小公倍数Ｌとを基に、次の合同式の条件からｄを求める。

$$e \times d = 1 \pmod L \quad \cdots (4)$$

即ち、

$$M=C^d=M^{ed}\ (mod\ n) \quad \cdots (5)$$

の条件が成立するように秘密鍵ｄを求める。

【００１８】前述のようにして、暗号化鍵（ｅ，ｎ）と復号鍵（ｄ，ｎ）とを求めることができる。そして、加入者１３の契約時等に於いて、この秘密鍵ｄを再生・記録装置１８の復号化部２５に設定しておくものである。又サービスセンタ１１の公開鍵処理部２０は、予め加入者の秘密鍵対応に公開鍵ｅ，ｎを格納しておき、リクエスト受付部２１により受付けた加入者の番号等を共に公開鍵ｅ，ｎを読出して暗号化部１５に加えることができる。暗号化部１５では、蓄積部１４から読出したデータに対して（1）式に従った暗号化を行うことになる。

【００１９】又再生・記録装置１８は、選択処理部２３と、カセットテープや磁気ディスク等の記録，再生可能の媒体を有する記憶部２４と、暗号化データを復号する復号化部２５と、ディスプレイや印字等の機能を含む再生部２６と、サービスセンタ１１に対してリクエストを送出する為のリクエスト送信部２７とを含む構成を有する。従って、受信した暗号化データは、再生部２６に於いて再生表示する時のみ、復号化部２６に於いて秘密鍵ｄを用いた復号鍵（ｄ，ｎ）によって復号することができる。

【００２０】又ネットワーク１２は、サービスセンタ１１や複数の加入者１３を収容し、交換機能を含む複数のノード１６と、ノード１６間を接続する回線とを含み、ノード１６間では多重化伝送を行う場合が一般的となる。又光信号によって多重化データを伝送する構成とすることもできる。

【００２１】前述のように、加入者１３がネットワーク１２を介してサービスセンタ１１にアクセスし、サービスセンタ１１からの応答によって、リクエスト送信部２７からサービスセンタ１１にデータ名や加入者番号等を用いてリクエストすると、サービスセンタ１１ではリクエスト受付部２１に於いて受付け、蓄積部１４からリクエストに従ったデータを読出し、公開鍵処理部２０から加入者１３の秘密鍵に対応する公開鍵を暗号化部１５に加えて、データを暗号化し、送信部２２からネットワーク１２を介して加入者１３に暗号化データを送出する。

【００２２】加入者１３は、受信装置１７によってネットワーク１２を介した暗号化データを受信し、加入者の入力操作によって選択処理部２３は、記録部２４に加えて暗号化データを記録するか、又は復号化部２５に加えて復号して再生部２６に加えるかを選択する。記録部２４には暗号化データが記録されるから、例えば、カセットテープ等によって構成した場合に、暗号化データを記憶したカセットテープを他の再生・記録装置に装着して再生しようとしても、復号化部２６に設定された秘密鍵が相違するから復号できないことになる。

【００２３】又受信装置１７に複数台の再生・記録装置を接続した場合も、再生・記録装置対応に秘密鍵が設定されるものであるから、記録部２４に受信した暗号化データを、リクエストを送出した再生・記録装置以外の装置で再生しようとしても、復号できないことになる。即ち、受信した暗号化データは、リクエストを送出した再生・記録装置１８に於いてのみ再生表示や再生印字が可能となり、それによって無断複製が防止され、著作権保護が可能となる。

【００２４】図３は本発明の実施例のノードの説明図であり、ネットワークとサービスセンタとの間のトラヒックを低減する場合の加入者収容のノード１６の構成を示す。同図に於いて、３１はコピー部、３２はコピー制御部、３３は暗号化部、３４は公開鍵処理部、３５はリクエスト受付部である。コピー部３１は、データをコピーして暗号化部３３に加えるもので、コピーが完了するまでデータを一時的に蓄積できる容量のメモリを備えている。

【００２５】図２に於ける加入者１３を収容したノード１６に、図３に示す構成を設けた場合、このノード１６に収容された加入者１３からのリクエストに対して、サービスセンタ１１では、暗号化部１５に於けるデータの暗号化を中止し、蓄積部１４から読出したデータをそのまま送信部２２から送出する。又ネットワーク１２の加入者を収容した総てのノード１６にコピー部３１や暗号化部３３等の構成を備えた場合は、サービスセンタ１１の暗号化部１５を省略することができる。

【００２６】加入者が複数台の再生・記録装置を備えて、同一のデータをサービスセンタに対してリクエストした場合、ノードのリクエスト受付部３５でリクエスト数を保持し、サービスセンタに対してはデータ名等のリクエストのみを送出する。サービスセンタは、このリクエストに従ったデータを蓄積部１４から読出し、暗号化しないで送信部２２から送出する。

【００２７】加入者を収容したノードでは、リクエスト受付部３５からコピー制御部３２に、リクエストした加入者番号等とリクエスト数とを通知し、コピー制御部３２はコピー部３１を制御して、サービスセンタからのデータをリクエスト数だけコピーし、又コピー制御部３２は加入者番号等に対応した秘密鍵に対応する公開鍵を公開鍵処理部３４から暗号化部３３に加え、リクエストされたデータをそれぞれ暗号化して送出する。

【００２８】例えば、図１に示す加入者３－１のように、複数台の再生・記録装置８を有する場合に、複数の同一データのリクエストを行った場合、単一の加入者３－１の番号のみでなく、複数台の再生・記録装置８についての情報をそれぞれ所定の順序で送出し、ノードのコピー制御部３２は、その送出順序に従って公開鍵を公開鍵処理部３４から暗号化部３３に加えて暗号化し、加入

者３－１では、受信順序に従って暗号化データを各再生・記録装置８に順次分配し、自再生・記録装置に於いてのみ復号できるデータを受信処理するように構成することができる。

【００２９】従って、複数のデータのリクエストがあっても、同一のデータについては、サービスセンタとネットワークとの間では１データの転送のみで済むから、サービスセンタの処理負担の軽減とネットワークのトラヒックの低減とを図ることができる。

【００３０】図４は本発明の実施例のサービスセンタとノードとの説明図であり、加入者を収容したノードは、コピー部４１とコピー制御部４２と暗号化部４３と公開鍵処理部４４とを備え、サービスセンタ４５は、各種データを蓄積した蓄積部４６と加入者からネットワークを介したリクエストを受付けるリクエスト受付部４７を備えている。

【００３１】サービスセンタ４５のリクエスト受付部４７は、単一の加入者からの複数の同一データのリクエスト又は複数の加入者から同一のデータのリクエストがあった場合、蓄積部４６からそのデータを検索して読出して送出し、且つリクエスト数及び加入者番号等の情報を送出する。加入者を収容したノードは、コピー部４１にデータが加えられ、リクエスト数及び加入者番号等の情報がコピー制御部４２に加えられる。

【００３２】コピー制御部４２は、リクエスト数に従ってコピー部４１を制御して、サービスセンタからのデータをコピーし、暗号化部４３に加える。又公開鍵処理部４４を制御して、加入者対応又は再生・記録装置対応の秘密鍵に従った公開鍵を暗号化部４３に加える。従って、暗号化部４３は、コピーしたデータ対応に公開鍵処理部４４からの公開鍵で暗号化し、加入者に送出する。

【００３３】この実施例に於いても、サービスセンタの処理負担を軽減し、且つネットワークとの間のトラヒックの低減を図ることができる。又ノードは、サービスセンタからの指令に従ってデータのコピー等を行うものであるから、比較的簡単な構成で実現できる。又サービスセンタに於いてリクエスト数を把握して課金処理等を容易に行うことができる利点がある。

【００３４】

【発明の効果】以上説明したように、本発明は、加入者３－１～３－ｎに於ける再生・記録装置８対応に、予め秘密鍵を復号化部９に設定し、再生時のみ復号化部９で復号する構成とし、サービスセンタ１に対してリクエストしたデータは、ネットワーク２を介して秘密鍵に対応した公開鍵で暗号化するから、加入者３－１～３－ｎ側で無断で複製したとしても、他の再生・記録装置８に於いては秘密鍵が異なるから復号できないことになる。従って、著作権の問題を解決することができる。

【００３５】又加入者３－１～３－ｎを収容したネットワークのノード６に、データのコピー機能と暗号化機能とを設けて、同一のデータに対する複数のリクエストに対して、サービスセンタ１は単一のデータをノード６に転送し、ノード６に於いてリクエスト数に従ったデータ数にコピーし、且つそれぞれ加入者３－１～３－ｎの再生・記憶装置８の秘密鍵に対応する公開鍵で暗号化して加入者に送出するもので、サービスセンタ１の処理負担を軽減し、且つネットワーク２のノード６との間のトラヒックを低減することができる利点がある。

【００３６】又サービスセンタ１に於いて、リクエスト送出の加入者及び同一のデータのリクエスト数を管理し、加入者３－１～３－ｎを収容したネットワーク２のノード６に、リクエストに対応したデータとリクエスト数とを送出し、ノード６は、サービスセンタ１から通知されたリクエスト数に従ってデータをコピーし、それぞれ加入者の秘密鍵に対応する公開鍵で暗号化して送出するもので、サービスセンタ１とネットワーク２のノード６との間のトラヒックを低減すること共に、サービスセンタ１に於いて加入者のリクエスト管理が可能となり、課金等の処理も容易となる利点がある。

【図面の簡単な説明】

【図１】本発明の原理説明図である。

【図２】本発明の実施例の説明図である。

【図３】本発明の実施例のノードの説明図である。

【図４】本発明の実施例のサービスセンタとノードとの説明図である。

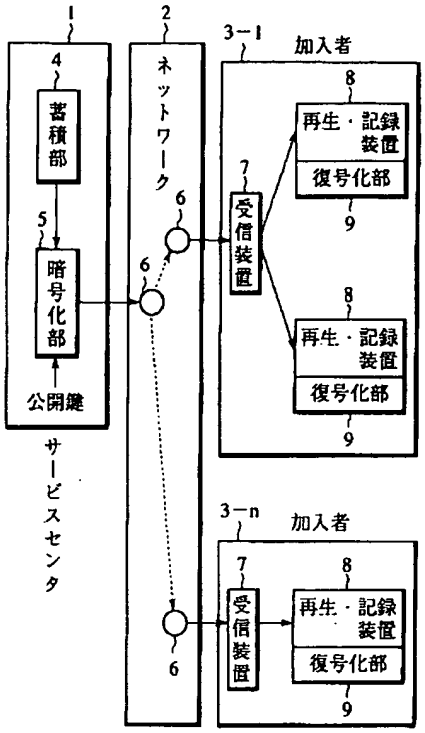
【図５】従来例の説明図である。

【符号の説明】

１　サービスセンタ
２　ネットワーク
３－１～３－ｎ　加入者
４　蓄積部
５　暗号化部
６　ノード
７　受信装置
８　再生・記録装置
９　復号化部

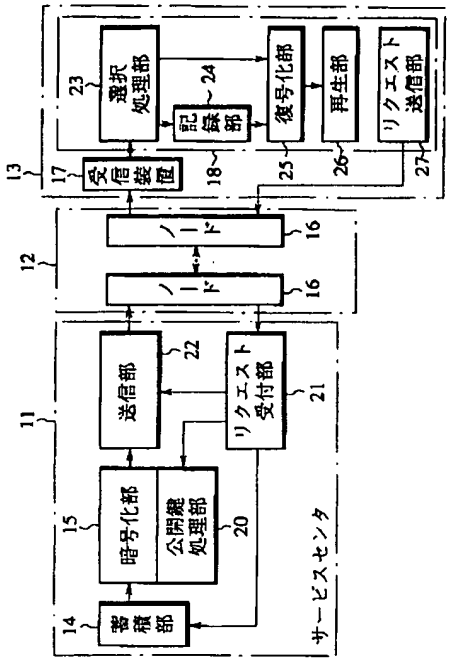
【図１】

本発明の原理説明図



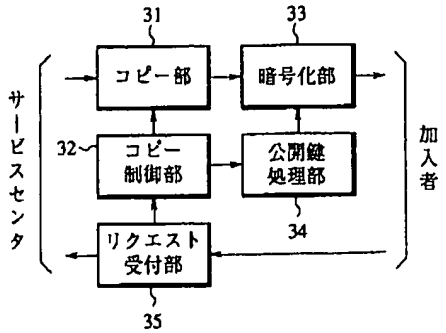
【図２】

本発明の実施例の説明図



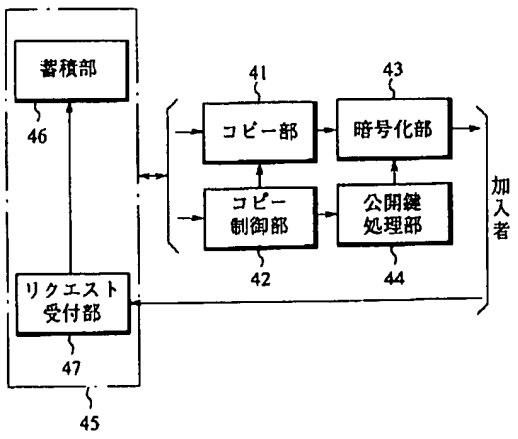
【図３】

本発明の実施例のノードの説明図



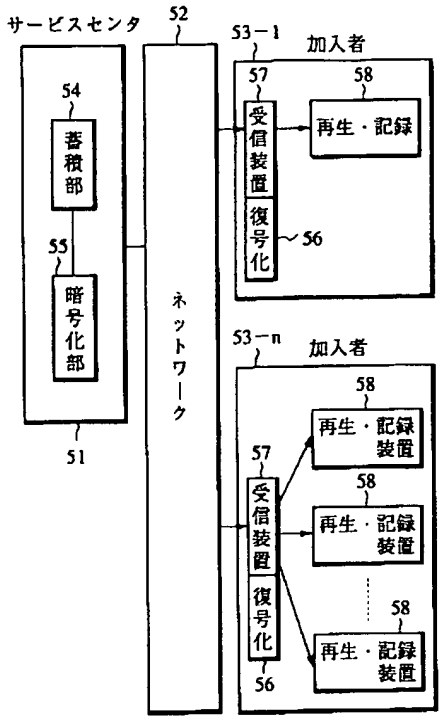
【図４】

本発明の実施例のサービスセンタとノードとの説明図



【図５】

従来例の説明図



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/14				
12/54				
12/58				

(72)発明者　奥田　将人
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内